PROVINCIA AUTONOMA DI TRENTO

APPAG - Agenzia provinciale per i pagamenti
Via G. B. Trener, 3 – 38121 Trento - tel. 0461 494909
fax 0461 495595 - e-mail: siap@provincia.tn.it

Direzione

Politica generale di sicurezza informatica dell'Agenzia Provinciale per i Pagamenti

Versione 4.0

Indice generale

1.0 Introduzione

L'Agenzia Provinciale per i Pagamenti (di seguito anche APPAG o Agenzia) è stata istituita dalla legge provinciale 28 marzo 2003, n. 4 - art. 57. All'APPAG sono attribuite (ai sensi dei regolamenti (CE) n. 1290/2005 e n. 885/2006) le funzioni di organismo pagatore degli aiuti derivanti dalla politica agricola comune per la Provincia autonoma di Trento.

L'Agenzia provinciale per i pagamenti si articola in:

- Direzione e affari generali;
- Controllo interno:
- Ufficio Unità Informatizzazione e Sviluppo Piattaforme Informatiche;
- Unità Tecnica e di Autorizzazione Premi;
- Unità Tecnica e di Autorizzazione Investimenti;
- Unità di Esecuzione Pagamenti;
- Unità di Contabilizzazione.

Tale struttura organizzativa è stata definita in modo da garantire la separazione delle funzioni di autorizzazione, esecuzione e contabilizzazione dei pagamenti, nonché la costituzione di servizi di controllo interno e tecnico, così come stabilito nei criteri previsti per il riconoscimento dell'organismo pagatore dal Regolamento (UE) n. 1306/2013 del Parlamento Europeo e del Consiglio del 17 dicembre 2013 e dal Regolamento Delegato (UE) n. 907/2014 della Commissione dell'11 marzo 2014.

L'Allegato I, punto 3, lettera "B" del Regolamento Delegato (UE) n. 907/2014 recita:

B) Sicurezza dei sistemi d'informazione

i) Fatto salvo il punto ii) di seguito, la sicurezza dei sistemi d'informazione si basa sui criteri definiti in una versione applicabile, nell'esercizio finanziario di cui trattasi, di una delle seguenti norme:

- *International Standards Organisation (Organizzazione internazionale per la standardizzazione) 27002: Code of practice for Information Security controls (ISO) (codice di buona pratica per i controlli sulla sicurezza delle informazioni).*
- *Bundesamt für Sicherheit in der Informationstechnik: IT-Grundschutzhandbuch/Manuale di sicurezza informatica di base (BSI).*
- *Information Systems Audit and Control Association: Control Objectives for Information and related Technology (COBIT) (obiettivi di controllo nel campo dell'informazione e delle tecnologie correlate.*

ii) A decorrere dal 16 ottobre 2016 la sicurezza dei sistemi d'informazione è certificata in conformità con l'Organizzazione internazionale per la standardizzazione 27001: Sistemi di gestione della sicurezza delle informazioni — Requisiti (ISO).

La Commissione può autorizzare gli Stati membri a certificare la sicurezza dei loro sistemi d'informazione in conformità con altre norme riconosciute se tali norme garantiscono un livello di sicurezza almeno equivalente a quello previsto dalla norma ISO 27001.

Per gli organismi pagatori responsabili della gestione e del controllo di una spesa annuale dell'Unione non superiore a 400 milioni di EUR, gli Stati membri possono decidere di non applicare le disposizioni di cui al primo comma. In tale caso, gli Stati membri continuano ad applicare le disposizioni di cui al punto i). Essi comunicano la loro decisione alla Commissione.

Con riferimento alla previsione del predetto Regolamento, APPAG, in quanto responsabile della gestione e del controllo di una spesa annua inferiore a 400 milioni di euro, ha comunicato, per il tramite dell'Organismo di Coordinamento AGEA, alla Commissione UE, che intende avvalersi della facoltà di non applicare quanto previsto dal p.to 3 (B) (ii) dell'Allegato I del Regolamento Delegato (UE) n. 907/2014, ma che continuerà ad applicare quanto previsto dal p.to 3 (B) (i) dello stesso Allegato I al Regolamento Delegato (UE) n. 907/2014.
APPAG, ha scelto a suo tempo, lo standard ISO 27002: Codice di Buona Pratica per i Controlli sulla Sicurezza delle Informazioni, quale norma internazionale di riferimento per la gestione della sicurezza dei propri sistemi informativi.

2.0 Ambito di applicazione

Con la legge provinciale 27 luglio 2012, n. 16 (Disposizioni per la promozione della società dell'informazione e dell'amministrazione digitale e per la diffusione del software libero e dei formati di dati aperti) è stato istituito il sistema informativo elettronico trentino (SINET). Il SINET sostituisce il pre-esistente Sistema Informativo Elettronico Provinciale (SIEP).
La gestione del sistema informativo elettronico provinciale è affidata in concessione ad Informatica Trentina SpA, società a prevalente capitale pubblico. I rapporti dipendenti dalla concessione sono regolati con apposita convenzione.
APPAG, quale struttura della Provincia autonoma di Trento, si avvale di tutti i servizi che, ai termini della convenzione tra Provincia autonoma di Trento e Informatica Trentina SpA, la società eroga. Tutti gli asset relativi sono gestiti dalla Società anche per conto di APPAG.
In sostanza, tutta la gestione dell'informazione di APPAG avviene a cura di Informatica Trentina SpA, ad eccezione di una piccola parte di documentazione cartacea che è gestita direttamente.

Questa politica generale di sicurezza costituisce un quadro di riferimento che deve essere applicato:

- da APPAG;
- da tutte le strutture della Provincia autonoma di Trento ed altri enti/società delegate che sono coinvolte dall'attività dell'Agenzia;
- da Informatica Trentina in quanto responsabile della gestione del SINET;
- da tutti i responsabili esterni dei trattamenti di cui si avvale APPAG.

Questo documento, approvato dalla Direzione di APPAG, è stato predisposto dall'Ufficio Unità Informatizzazione e Sviluppo Piattaforme Informatiche in accordo con le prassi e gli indirizzi di Informatica Trentina S.p.A. e della struttura provinciale competente in materia di informatica.
Di seguito sono individuati i principali ruoli e le principali responsabilità di carattere decisionale previsti per la gestione della sicurezza delle informazioni in ambito IT che APPAG tratta nell'esercizio delle proprie funzioni istituzionali.

3.0 Individuazione dei ruoli

3.1 Provincia Autonoma di Trento

APPAG si configura come struttura provinciale e quindi, ai sensi della normativa in materia di protezione dei dati – ed in particolare di quanto disciplinato dal Reg. UE 2016/679 del Parlamento Europeo e del Consiglio, del 27 aprile 2016, nonché del D.lgs 10 agosto 2018 n. 101 avente ad oggetto "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Reg. UE 2016/679 del Parlamento UE e del Consiglio del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali

dati e che abroga la direttiva 95/46/CE" - la stessa, adotta per quanto riguarda la classificazione delle informazioni e dei dati, la valutazione del rischio e le conseguenti modalità di gestione, le modalità operative previste dalla stessa Provincia autonoma di Trento. I documenti che le descrivono, sono disponibili direttamente sul sito della Provincia Autonoma di Trento, al seguente indirizzo http://172.17.2.3/tratt/.

3.2 Dirigente della struttura competente in materia di informatica

Al Dirigente della struttura competente in materia di informatica spettano l'individuazione di specifiche istruzioni operative a garanzia della sicurezza, ad integrazione e chiarimento di quelle stabilite dalla Giunta provinciale e l'assistenza tecnica alle strutture in ordine all'applicazione delle misure di sicurezza per il trattamento dei dati personali gestiti a livello informatico.

3.3 Direttore dell'Agenzia Provinciale per i Pagamenti

Spettano al Direttore di APPAG le funzioni che hanno a che fare con decisioni e scelte attinenti l'attività gestionale e la vigilanza sull'applicazione delle misure di sicurezza da parte del personale assegnato alle strutture di propria competenza.

Qualora il Direttore lo ritenga opportuno, al fine di rispettare gli standard derivanti dalla normativa comunitaria e nazionale in materia di organismi pagatori, può adottare ulteriori misure di sicurezza.

3.4 Informatica Trentina S.p.A. - Responsabile della gestione del SINET

L'amministratore di sistema è il soggetto cui è conferito il compito di sovrintendere alle risorse di un sistema informativo elettronico e di consentirne l'utilizzazione.

La Giunta provinciale, con propria deliberazione n. 1081 del 7 giugno 2013, ha nominato Informatica Trentina S.p.A. responsabile del trattamento dei dati della Provincia alla stessa affidati ai sensi della L.P. 6 maggio 1980 n. 10 (Legge istitutiva del SIEP, ora SINET).

Poiché tutte le risorse assegnate al SINET, compresi i sistemi in uso presso APPAG: SIAP, SR-Trento, SOC, sono gestiti da Informatica Trentina SpA, spettano alla stessa Società ed ai soggetti da essa preposti le funzioni di controllo e coordinamento che non sono riservate ai responsabili delle strutture provinciali, in quanto responsabili dei trattamenti anche ai sensi del Reg. UE 2016/679 del Parlamento Europeo e del Consiglio, del 27 aprile 2016, nonché del D.lgs 10 agosto 2018 n. 101 avente ad oggetto "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Reg. UE 2016/679 del Parlamento UE e del Consiglio del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE".

Le indicazioni generali del presente documento si applicano, di conseguenza, anche a Informatica Trentina SpA.

Informatica Trentina SpA, possiede un Sistema di Gestione per la Sicurezza delle Informazioni certificato in conformità ai requisiti della norma UNI CEI ISO/IEC 27001, per il seguente campo applicativo: "Progettazione, realizzazione, avviamento ed erogazione continuativa di servizi applicativi, tecnologici, di sicurezza e di formazione erogati alle Amministrazioni trentine, ed esecuzione delle attività di supporto che consentono ad Informatica Trentina l'erogazione degli stessi".

3.5 Utenti

Gli utenti condividono le responsabilità per la protezione delle risorse loro affidate, incluse le

informazioni e gli strumenti informatici. Tutto il personale deve essere accuratamente informato sulle politiche di sicurezza adottate e deve prontamente evidenziarne ogni violazione, anche sospetta, al proprio responsabile.

4.0 Principi di sicurezza

Premesse le indicazioni prima fornite relativamente ai ruoli dei soggetti coinvolti nella gestione delle informazioni in ambito IT, che interessano l'attività di APPAG, si riportano di seguito i **principi generali**, *(in conformità a quanto stabilito dalla* ***standard ISO 27002****: Codice di Buona Pratica per i Controlli sulla Sicurezza delle Informazioni),* che definiscono la **Politica di gestione della sicurezza delle informazioni in ambito IT,** adottata da APPAG.

4.1 Organizzazione della sicurezza

L'implementazione ed il controllo della sicurezza dei dati e delle informazioni gestiti in ambito IT, all'interno di APPAG devono essere regolamentati ed organizzati.
In particolare i soggetti coinvolti (interni ed esterni), in funzione dei compiti assegnati, devono provvedere a:

- definire, approvare e applicare le politiche di sicurezza e le relative procedure;
- definire le modalità di valutazione dei rischi e la scelta delle contromisure per la loro riduzione;
- implementare dei controlli di sicurezza idonei, in funzione dei rischi concretamente rilevati;
- monitorare la correttezza e l'efficacia del sistema di controllo implementato.

4.2 Inventario e classificazione delle risorse

Le risorse informatiche utilizzate a supporto delle attività, indipendentemente dal tipo, dal formato e dai supporti di memorizzazione o di comunicazione, devono essere gestite al fine di preservarne la riservatezza ed integrità.
Da tale principio consegue che deve essere:

- predisposto e mantenuto un inventario dei beni/risorse;
- individuato un proprietario/utente per ogni bene/risorsa;
- classificato ogni bene/risorsa al fine di permettere l'adozione di misure di sicurezza commisurate al valore del bene/risorsa stesso/a.

4.3 Personale

Il personale coinvolto nella gestione delle informazioni gestite in ambito IT, è parte attiva del processo di gestione del rischio di sicurezza e quindi deve essere a conoscenza della politica generale della sicurezza e delle procedure di sicurezza adottate. Ne consegue che il personale deve:

- essere informato circa le proprie responsabilità in tema di sicurezza;
- essere adeguatamente formato e sensibilizzato, secondo appositi piani di formazione in funzione dei ruoli e delle responsabilità di sicurezza attribuiti, per il rispetto puntuale dei principi e l'applicazione delle regole adottate ed operare seguendo scrupolosamente le regole di sicurezza definite, facendosi portatore nei confronti della dirigenza di suggerimenti e richieste;
- segnalare ogni incidente o sospetto tale e ogni comportamento non in linea con quanto definito, secondo le procedure di comunicazione predisposte.

4.4 Sicurezza fisica

I beni/risorse IT, devono essere protetti tramite la predisposizione e il mantenimento di un ambiente fisico che impedisca la loro perdita o fuoriuscita ed il loro danneggiamento.
Tale principio deve essere perseguito attraverso misure di controllo, correlate ai rischi e al valore dei beni/risorse.
Ne fanno parte le seguenti componenti:

- la definizione e la classificazione dei perimetri di sicurezza;
- l'implementazione di misure di sicurezza negli ambienti definiti;
- il corretto posizionamento delle risorse fisiche all'interno dei perimetri in relazione alla classificazione di sicurezza;
- la tempestiva rilevazione di eventi anomali.

4.5 Gestione operativa e delle comunicazioni

L'infrastruttura tecnica deve essere gestita in modo efficace ed efficiente nel tempo al fine di garantire che all'utente sia fornito il livello di servizio richiesto e che i beni/risorse (materiali e immateriali) siano gestiti, anche nel trasferimento, in modo da preservarne la riservatezza e la criticità. Pertanto:

- gli aggiornamenti dell'hardware, del software di base e degli applicativi devono essere pianificati e autorizzati al fine di minimizzare gli impatti sul livello di servizio;
- le procedure di autorizzazione e di implementazione devono essere rispondenti ai differenti requisiti di sicurezza e di continuità in relazione alla diversa tipologia di intervento;
- la gestione dei cambiamenti deve essere disciplinata da apposita procedura, inserita e gestita nel sistema di gestione della sicurezza informatica;
- i test di modifiche strutturali o evolutive devono essere effettuati in un ambiente dedicato a tale scopo.

A questo proposito, il processo di collaudo del software deve essere condotto secondo le specifiche di test:

- i dati di produzione non devono essere utilizzati per scopi di test senza che ogni informazione riservata e ogni dato personale sia prima rimosso o modificato in modo da preservare i dati stessi;
- gli incidenti (malicious software, virus, etc.) devono essere gestiti tramite procedure formalizzate;
- il trasferimento e la comunicazione delle risorse informatiche devono essere normate tramite apposite procedure documentate.

4.6 Controllo accessi logici

La sicurezza deve essere un elemento costitutivo nella fase di sviluppo e di progettazione di nuovi prodotti/sistemi/servizi di APPAG e i prodotti/servizi, sviluppati da o per conto della stessa, devono rispettare requisiti di sicurezza definiti sulla base di una specifica analisi dei rischi, pertanto:

- l'accesso alle risorse informatiche deve essere autorizzato formalmente in base alle reali esigenze operative;
- la gestione delle credenziali degli utenti e dei loro profili di accesso alle risorse devono essere definite tramite procedure, supportate da appositi strumenti software e/o hardware;
- gli utenti autorizzati devono essere responsabilizzati all'osservanza delle procedure e delle misure di sicurezza definite.

4.7 Progettazione e sviluppo prodotti/servizi

La disponibilità dei servizi erogati deve essere garantita, in funzione della loro criticità, al fine di assicurare il ripristino dei processi critici entro termini tollerabili, per quanto riguarda l'operatività sia interna sia esterna. Durante le fasi di sviluppo e di progettazione di nuovi prodotti/sistemi/servizi devono essere eseguite le seguenti attività:

- per i prodotti/sistemi/servizi che richiedano un elevato livello di sicurezza, deve essere svolta un'adeguata valutazione del rischio di sicurezza che porti alla definizione di controlli atti a diminuire il rischio;
- implementazione dei controlli organizzativi, procedurali e tecnologici necessari;
- gestione del sistema di sicurezza implementato, che comprenda anche la manutenzione correttiva ed evolutiva.

4.8 Continuità del servizio

Le misure di sicurezza organizzative, procedurali e tecnologiche a tutela della continuità del servizio devono essere formalizzate all'interno di una struttura documentale basata su un piano di continuità che preveda l'individuazione di:

- ruoli e responsabilità coinvolte nel mantenimento della continuità;
- criteri al fine di individuare i processi/servizi critici;
- requisiti di continuità.

Il piano inoltre deve fornire le linee guida in merito alle misure preventive (organizzative e tecnologiche) e alla procedura di escalation, sulla base dei livelli di gravità del danno emergente.

4.9 Conformità

Qualsiasi comportamento deve essere conforme alla normativa di legge inerenti l'ambito dei sistemi informativi e l'ambiente ICT nonché al trattamento di dati personali, alle disposizioni interne e deve essere verificato e garantito nel tempo.

Per conformità si intendono i seguenti adempimenti:

- adozione delle misure richieste per la protezione dei dati personali;
- definizione e documentazione dei requisiti normativi e contrattuali;
- adozione delle misure richieste per rispettare gli obblighi contrattuali sul copyright;
- conformità ai requisiti di legge delle registrazioni da presentare in contenziosi legali;
- adozione delle precauzioni necessarie per evitare l'uso illecito delle risorse di elaborazione e comunicazione.